(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2007-502554
(P2007-502554A)
(43)公表日 平成19年2月8日(2007.2.8)

(51)Int.Cl.		F I			テーマコード(参考)
H04L 12/69	(2006.01)	H04L	12/58	100Z	5K030

審査請求 未請求　予備審査請求 未請求　(全 23 頁)

(21)出願番号　特願2006-522001(P2006-522001)
(86)(22)出願日　平成16年7月28日(2004.7.28)
(85)翻訳文提出日　平成18年3月23日(2006.3.23)
(86)国際出願番号　PCT/US2004/024186
(87)国際公開番号　WO2005/015068
(87)国際公開日　平成17年2月17日(2005.2.17)
(31)優先権主張番号　10/627,672
(32)優先日　平成15年7月28日(2003.7.28)
(33)優先権主張国　米国(US)

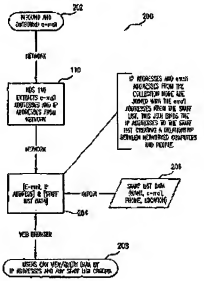
(71)出願人　506028454
エテレメトリー インク
アメリカ合衆国、２１４０１　メリーランド州、アナポリス、スート　２０１、オールド ソロモンズ アイランド ロード４３
(74)代理人　100104156
弁理士　龍華　明裕
(72)発明者　シュヌマン、アラン
アメリカ合衆国、２１４０１　メリーランド州、アナポリス、サンウッド レイン５０８

Fターム(参考)　5K030 GA11 HA05 KA06 MA04

最終頁に続く

(54)【発明の名称】ネットワーク化されたコンピュータのユーザを特定するネットワークアセットトラッカ

(57)【要約】
ネットワーク化されたコンピュータのユーザを特定する、ネットワークに付随する装置、システム、方法、及びコンピュータプログラム製品を提供する。この装置はコアネットワークアップリンクポイントに設置され、パケットがネットワークを通る際にパケットを解析し、トラフィックの内容をユーザコンタクト情報及びシステムアクセス情報にインテリジェントに相関付ける。得られた情報を用いて、ネットワーク化されたコンピュータのユーザをセキュリティ又は課金を目的として特定する。



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention]
[0001]
This invention relates to the device, the system, method, and computer program product which provide security in such a computer network especially about a computer network comprehensively.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[Field of the Invention]
[0001]
This invention relates to the device, the system, method, and computer program product which provide security in such a computer network especially about a computer network comprehensively.
[Background of the Invention]
[0002]
It is common that companies (namely, a trading company, a company, an organization, an organization, a government agency, etc.) own and employ one or more computer networks (for example, Local Area Network (LAN) etc.) in today's technical situation. Such computer networks may spread over some offices, a floor, and/or a building. A lot of pro PURAETARI (it is sometimes secrecy) data which requires prudent treatment is in such computer networks. Therefore, naturally such a company worries about the security of each one of computer networks.
[0003]
It is concerned with operation of login / password method, there is nothing, and it is inevitable that a denied user gets access to a computer network. even if it is the users (for example, an employee, an independent contract employee, a subcontractor, etc.) to whom access of the computer network is permitted, there is actually a possibility of it being alike occasionally, carrying out and using such a network with the form which is not approved. Many unauthorized actions (activity) are concentrating on the E-mail ("E-mail"). For example, there is a possibility that the authority user who is acting with the denied user or the form which is not approved may transmit to the computer system which has not received people who have not received approval for the security data of the company using E-mail, or approval via the public Internet of a worldwide scale.
[Description of the Invention]
[Problem(s) to be Solved by the Invention]
[0004]
The device, the system, method, and computer program product which specify the user of the computer connected by network from the above-mentioned problem are required. This problem is overcome today, when either generally follows a cable physically to a physical location first with reference to the existing cable plant documentation (supposing it is). Subsequently, a security staff or IT staff has to go to the physical location, and has to specify a violation user physically. However, the device, the system, method, and computer program product which are needed, A network E mail traffic should be analyzed and the Internet Protocol (IP) address should be mapped in the end user (that is, specific in the user of the specific IP address in a network). Probably the device, the system, method, and computer program product which are needed specify the computer which threatens security, and will shorten the response time at the time of pinpointing and disabling the position.
[Means for Solving the Problem]
[0005]

This invention fulfills necessity specified in a top by providing a device, a system, a method, and a computer program product which specify a user of a computer connected by network. That is, in one embodiment, this invention provides a network asset tracking system which maps an end user to a workstation Internet Protocol (IP) address by analyzing network traffic (it exists) passively. In one embodiment, a report of mapping to an IP address from an end user also provides a network asset tracking system of this invention via a Web site application supported by database.

[0006]

According to one embodiment, a network asset tracking system of this invention is provided with two components "back end", i.e., a name discovery system, and a management Web site application "front end." A name discovery system ("NDS") is a "Sniffer" device (namely, hardware) connected to a primary switch of company LAN. An NDS device catches and analyzes network traffic. Since an administrator of a computer network performs management of data and correlation attachment which were caught by NDS, and does cross correlation of such data to directory data of a company and an IP address is mapped in an end user, a Web site application is provided.

[0007]

An advantage of this invention is to enable it to specify a computer user who shortens response time at the time of pinpointing and disabling a position of a computer with doubt, and threatens security.

[0008]

Another advantage of this invention maps a computer user's identity in directory information (for example, a building, a room, a telephone, etc.) of an organization, and is in a thing for which a physical location of a computer can be traced (that is, a specific building and/or a room are pinpointed) and which are made like. Therefore, as a security threat which this invention copes with, what [not only] is depended on a denied user but a Trojan horse type attack in which it is very important performing offensive position specification physically is included.

[0009]

There is another advantage of this invention in the ability to specify an organization of a computer user and a computer user in a company for specifying a computer user who is using a computer network asset unsuitably, and the information technology (IT) infrastructure fee collection purpose. Although this advantage shares a big common network infrastructure, it becomes clear by a case where a fee collection problem which a major company which tries to assign a separate operation division or a section network maintenance and cost of a support faces is considered.

[0010]

There is another advantage of this invention in the ability to specify an error of existing cable plant (network) documentation. By connecting a physical location of network connection to an IP address on a switch port in a network closet, and providing it, This invention documents the last "hop" and enables it to inspect such existing network documentation.

[0011]

It explains in detail below, referring to an accompanying drawing for the further feature of this invention, an advantage, structure of various embodiments of this invention, and operation.

[0012]

The feature and an advantage of this invention will become clear from detailed explanation described below by a case where combine with a drawing and it interprets.

[Best Mode of Carrying Out the Invention]

[0013]

I. General view

This invention is aimed at the device, the system, method, and computer program product which specify the user of the computer connected by network.

[0014]

According to one embodiment, a company is provided with this invention as a solution for mapping an Internet Protocol (IP) address to the staff of an organization using the contents of directory data and network traffic. By installing a name discovery system unit (namely, "NDS" hardware) in the 1st at the

primary switch of the Local Area Network (LAN) of a company, The Local Area Network traffic (for example, Ethernet (registered trademark), FDDI, etc.) of a company is caught and analyzed. The caught data is mapped in correlation attachment **, and an IP address is mutually mapped in an end user with list data. The network asset tracking solution of this invention lets the Web site application supported by the database pass, and also provides [2nd] access and operation of network traffic data which were collected so that IT administrator member of a company may use it.

[0015]

The device of this invention, a system, a method, and a computer program enable it to specify the computer user who shortens the response time at the time of pinpointing and disabling the position of a computer with doubt, and threatens security. A company enables it for this invention to perform an accounting function again. A company billing and for the purpose of [other] fee collection (for example, share/assignment network infrastructure cost model which specific companies, such as a government organization, adopt) For example, a computer user's subset. It is interesting to search for the network operating condition (for example, the number of network connection) of (a subcontractor versus an employee [for example,]).

[0016]

This invention is explained in detail below about the above-mentioned example from this. This is for an expedient chisel and there is no intention which limits application of this invention. If the following explanation is read, the method of enforcing by the embodiment (for example, analysis of the network traffic of a different kind in a computer network of a different kind) of substitution for the following this inventions will actually be clear to a person skilled in the art.

[0017]

The plural of the term of a "user", a "company", a "staff", the "staff", an "organization", and a "company" and these terms is used for homonymy through this whole specification, People who access the tool provided since the user of the computer by which this invention was connected by network is specified, who use a tool and who are specified by a tool and will receive the benefit of/or a tool are pointed out.

[0018]

II. Structure of a device and a system

With reference to drawing 1, the network asset tracking ("NAT") system 100 by one embodiment of this invention is shown.

[0019]

The system 100 contains the Local Area Network (for example, Ethernet (registered trademark)) backbone 102 of the company which connects two or more end user computers 104 mutually. In a substitute embodiment, the computer 104 A terminal, a workstation. Sun(registered trademark) Solaris (trademark) and Microsoft(registered trademark) Windows2000 (trademark) -- or, [for example,] [XP and (trademark)] Or the Sun(registered trademark) SPARC (trademark) workstation, NT (trademark) workstation, or the personal computer (PC) (for example) which is running the IBM(registered trademark) AIX (trademark) operating system IBM (trademark) which is running Microsoft(registered trademark) Windows 95/98 (trademark), or a Windows NT (trademark) operating system, or compatible PC, It is the Macintosh (registered trademark) computer etc. which are running the Mac(registered trademark) OS operating system. (In order to simplify, computer 104 a-n is shown in drawing 1). According to a substitute embodiment, the user can access LAN102 using the arbitrary processing units 104 which are not limited to these, although a desktop computer, laptop, a palm top, a set top box, a personal information terminal (PDA), etc. are mentioned.

[0020]

The backbone of LAN102 is connected to the primary switch (namely, primary Internet link of LAN) 106. The switch 106 is connected to the router 108 and the router 108 provides the user of the computer 104 with connection with the public global Internet 112.

[0021]

According to one embodiment, the name discovery system ("NDS") device 110 is connected to the

primary switch 106. NDS110 functions as "Sniffer" hardware (namely, collection node) which catches the inbound outbound traffic of LAN102.

[0022]

In one embodiment, NDS110 is 1 rack unit (1U) box provided with the power source plug. According to such an embodiment, NDS110 has two 100Mbps network connection to the primary switch 106. As shown in drawing 1, one link is a mirrored rise ring which collects the data from LAN102 via one port of NDS110. The 2nd port of NDS110 is used in order to enable it to usually access via a Web site application, while transmitting a data file periodically. If explanation of this specification is read, in such an embodiment, two effective IP addresses are required for NDS110 so that I may be understood by the person skilled in the art. If this also reads explanation of this specification, when a network scale is larger, by a substitute embodiment, NDS110 can be installed in each core network uplink point (namely, primary switch), so that I may be understood by the person skilled in the art.

[0023]

According to one embodiment, the administrator of LAN102 can access NDS110 via the "front end" Web site application containing login / password method. Such a front end is provided by web server computer 114 which has the LAN102 connection with NDS110. The web server 114 provides the "front end" of the NAT system 100 so that I may be understood by the person skilled in the art. That is, the server 114 includes the web server process which answers the HyperText Transfer Protocol (HTTP) demand from a remote browser (for example, administrator of LAN102), or a HyperText Transfer Protocol (HTTPS) demand, and sends out a web page. More specifically, such Manage User of the NAT system 100 is provided with the graphical user interface (GUI) "front end" screen of the gestalt of a web page. A GUI picture is made to display that such web pages are transmitted to each computer 104 of a user.

[0024]

According to a substitute embodiment, the administrator of LAN102 can also remote access NDS110 via the secure shell (SSH) program on the port 22 of NDS110.

[0025]

In a substitute embodiment, NDS110 can be provided with the central repository which memorizes all the traffic data of LAN102 in which it was collected in the NATS system 100, or can access this so that I may be understood by the person skilled in the art, if this also reads explanation of this specification. To such a repository, it is accessible also from a "front end" Web site application, and the administrator of LAN102 can perform statistical collection, the inspection of a report, etc.

[0026]

Below is provided with the component of the NAT system 100, and the more detailed explanation about the function.

[0027]

III. Operation

With reference to drawing 2, the flow chart which shows the data flow of the network asset tracking process 200 by one embodiment of this invention is shown.

[0028]

First, the inbound outbound E mail traffic data 202 (for example, an IP address and an E-mail address) in LAN102 is collected by NDS110 (namely, extraction), and is memorized. At one embodiment, NDS110 is a Tethereal ("dumping and analysis of network traffic") network protocol analyzer utility (it is developed as an open source of Unix and Windows, and). the bottom of a GNU general public utilization permission contract -- being available -- it is used and data is extracted from LAN102. According to a substitute embodiment, if this invention is read, NDS110 can extract data from LAN102 using other large available utilities (custom code logic, such as Snoop and Tcpdump) so that I may be understood by the person skilled in the art.

[0029]

Next, the web server computer 114 (the above-mentioned database support Web site application is provided) which has the LAN102 connection with NDS110, Since the user of the computer 104 in

LAN102 is specified, the staff directory information 206 of a company is connected to NDS110 collection data (that is, a user is mapped in an IP address). More specifically, the server 114 provides such Manage User of the NAT system 100 with GUI208 "front end" screen with the gestalt of a web page. Such web pages will display GUI picture 208, if transmitted to each computer of a user.
[0030]
The staff directory information 206 of a company is composed of one embodiment as a formatted database of the others containing the data about the staff (namely, staff to whom use of the computer 104 in LAN102 is permitted) of ITU-T X.500 or a company. In one embodiment, such a database is the text file divided with a comma or tab including the illustration field enumerated to Table 1.
[0031]
[Table 1]

企業人員ディレクトリ２０６のフィールド例
ファーストネーム
ラストネーム
ミドルネームのイニシャル
ニックネーム
別名
建物
部屋
永久的なＥメール
一時的なＥメール
ユーザ名
Ｅメールアドレス
所属／組織

[0032]
According to one embodiment, the NAT system 100 generates the output data file containing all the LAN102 traffic data collected with the periodical time interval (for example, during per hour, every day, every week, etc.). According to such an embodiment, the text data file divided by processing of the data in the NAT system 100 with the comma so that it might be easy to import for other software application products (for example, Microsoft(registered trademark) Excel etc.) is created. According to a substitute embodiment, the output data file of the NAT system 100 includes some or all of the illustration fields that was enumerated to Table 2.
[0033]
[Table 2]

NAT出力ファイルフィールド例
IPアドレス
ホスト名
ファーストネーム
ミドルネームのイニシャル
ラストネーム
Eメールアドレス
ロケーション
電話番号

[0034]
According to one embodiment, Web site application GUI picture 208 provides the capability to sort the result of the tabular format about the arbitrary fields returned from Table 2. Mapping of the user to the IP address obtained as the field from Table 2 which the output data file of NAT100 can actually be shown, and a result is dependent on the quality of the data seen in the staff directory 206 of a company so that I may be understood by the person skilled in the art, if this specification is read. If this also reads this specification, both Table 1 and 2 can be tied up using the E-mail address field common to both Table 1 and 2 so that I may be understood by the person skilled in the art.
[0035]
Please understand that drawing 2 emphasizes the function and other advantages of the NAT system 100, and it is shown for the purpose of an example only. . With the method of showing collection and processing of the data in the NAT system 100 in drawing 2, perform structure of this invention with an option. (For example, one or more data processing functions shown as what is performed by the web server 114 may be performed by NDS110, and the reverse is also the same) It is flexible enough so that things may be made, and it can constitute.
[0036]
VI. NDS data extraction
In one embodiment, NDS110 analyzes the port 25 of the switch 106 about a simple mail transfer protocol (SMTP), The port 110 of the switch 106 is analyzed about postoffice protocol-versions 3 (POP3) data, About Internet message access protocol-versions 4 (IMAP) data, an E-mail address and an IP address can be extracted from LAN102 traffic data by analyzing the port 143 of the switch 106.
[0037]
With reference to drawing 3 A, the flow chart which shows the data flow of the network asset tracking process 200 by one embodiment of this invention is shown. By drawing 3 A, NDS110 more specifically The internal (SMTP) mail server 302 and the exterior of a company. (For example, public Internet) The user of the computer 104 is specified from the SMTP data traffic 202 exchanged among the outside users 306 who have accessed the SMTP mail server 308.
[0038]
Not almost all equipment of an SMTP server carries out compression or encryption of data. The domain of E-mail dispatch origin is pinpointed by SMTP greeting the first stage. The extracted data 304 (namely, E mail traffic data which NDS110 extracted) is analyzed by the process 200 so that drawing 3

A may see. By a command "MAIL FROM:", a sending person's perfect E-mail address is specified, and an addressee's perfect E-mail address is specified by a command "RCPT TO:." If NDS110 extracts data from LAN102, it will look for the following patterns using the code logic memorized, and a user-identification child will be obtained.
Command:MAIL
Request parameter:FROM:
or
Command:RCPT
Request parameter:TO:
A user-identification child continues after "FROM:" and "TO:" in the state where it probably entered in "<" and the ">" character. ": The language after " and in front of "<" is usually a certain string of a user-identification child. ("FROM:" and "TO:" point out a sending person and an addressee, respectively).
[0039]
With reference to drawing 3 B, the flow chart which shows the data flow of the network asset tracking process 200 by one embodiment of this invention is shown. More specifically by drawing 3 B, NDS110 specifies the user of the computer 104 from the POP3 traffic 202 exchanged among the outside users who have accessed the internal (POP) mail server 302 and external (for example, public Internet) mail server of a company.
[0040]
A POP3 protocol does not use a data encryption or compression. As shown in drawing 3 B, the extracted data 304 (namely, E mail traffic data which NDS110 extracted) is analyzed by the process 200. In a space, in POP3, a user's identity (usually user name portion of an E-mail address) continues next following the "USER" command. As for almost all the embodiments (implementations) of POP3, the "PASS" command usually continues after the "USER" command. A space continues after the "PASS" command and, subsequently a user's password continues by a plaintext (namely, text which is not enciphered). A user's reliability is checked by the response "O.K." of a server. Therefore, at such an embodiment, analysis in the real time over a POP3 protocol is conducted by performing the following pattern matching using code logic.
Request:USER
Request Arg:
It continues after the user name string as whom "Request Arg:" specifies a user's identity. With this information, a packet header identifies clearly the system which the user is using including a sending agency IP address and destination IP addresses. The artificer found out that data required generally in order to catch a user's identifier was less than 64 bytes.
[0041]
With reference to drawing 3 C, the flow chart which shows the data flow of the network asset tracking process 200 by one embodiment of this invention is shown. More specifically by drawing 3 C, NDS110 specifies the user of the computer 104 from the IMAP traffic 202 exchanged between the internal (IMAP) mail server 302 of a company, and the outside user who has accessed external (for example, public Internet) E-mail.
[0042]
IMAP does not have a data encryption or compression by default like POP3, either. The extracted data 304 (namely, E mail traffic data which NDS110 extracted) is analyzed by the process 200 so that drawing 3 C may see. Therefore, a user's identity is specified using a string's "LOGIN" (with no distinction of a capital letter and a small letter) pattern matching. After the "LOGIN" command is published by the server, a user's identity is checked by the response "OK LOGIN completed" or "FAIL." It is a pattern to obtain the user name for a user's IMAP systems. :
Request Tag:000A
Request:LOGIN
[0043]
It is the same as that of the case of POP3 by investigation ******. After a keyword "LOGIN", two

arguments (a user name and a password) surrounded by double quotes continue. Extracting only the user name which is required information is performed at this step. The artificer found out like POP3 that the data which needs to be caught in order to obtain a user-identification child was less than 64 bytes. According to a client, a LOGIN command is usually in five IMAP packets of the beginning transmitted.
[0044]
With reference to drawing 3 D, the flow chart which shows the data flow of the network asset tracking process 200 by one embodiment of this invention is shown. By drawing 3 D, more specifically The internal (Exchange) mail server 302 and the exterior of a company. (For example, public Internet) The user of the computer 104 is specified from the Microsoft(registered trademark) ExchangeE mail data traffic 202 exchanged among the outside users 306 who have accessed E mail server (not shown in drawing 3 D).
[0045]
Microsoft(registered trademark) Exchange Server 2000 and the continuing updated version, Traffic is enciphered between the Microsoft(registered trademark) Outlook client (it performs on the client computer 104), and the Exchange mail server 302. Therefore, in the embodiment of substitution of this invention, the extracted data 304 is obtained using the small script loaded to the Exchange server 302. That is, a script is performed at the fixed interval constituted beforehand, and uses Exchange Server 2000 Message Tracking Center (.). namely, the server 302 top -- a message tracking feature -- enabling. E-mail's in a network the IP address and E-mail address of a sending person are extracted using the related tracking log file (for example, yyyymmdd.txt) which resides in the shared resource of the server 302 permanently.
[0046]
In a substitute embodiment, to a Microsoft Exchange tracking log file. A log file can be opened using a file system object, and it can remote access using the script which analyzes the syntax of a log file and obtains an E-mail sending person's IP address and E-mail address in a network.
[0047]
As it ranks second and the extracted data 304 was mentioned above by all of the two above-mentioned embodiments so that drawing 3 D might see, it is analyzable by the process 200. Since the above-mentioned embodiment of two substitution will use an Exchange log file so that I may be understood by the person skilled in the art of a pertinent art if explanation of this specification is read, in such an embodiment, NDS110 can be kept not used.
[0048]
Drawing 3 A - drawing 3 D should emphasize the function and other advantages of the NAT system 100, and should understand being shown for the purpose of an example, only. The structure of this invention of the method of showing collection and processing of the data in the NAT system 100 in drawing 3 A - drawing 3 D is flexible enough so that it can carry out with an option, and it can be constituted.
[0049]
V. The example of an embodiment
This invention (the system 100, the process 200, its arbitrary part (plurality is good), or a function (plurality is good)), It can carry out using hardware, software, or such combination, and can mount in one or more computer system or other processing systems. By one embodiment, this invention is actually aimed at one or more computer systems which can perform the function described in this specification. The example of the computer system 400 is shown in drawing 4. The computer system 400 is provided with one or more processors of processor 404 grade. The processor 404 is connected to the telecom infrastructure 406 (for example, a communication bus, a crossover bar, or a network). Various software embodiments are described in relation to this illustration computer system. If this explanation is read, the method of carrying out this invention using other computer systems and/or structures will become clear in a person skilled in the art.
[0050]
the computer system 400 can be provided with graphics, a text, and the display interface 402 that

transmits other data from the frame buffer which is not illustrated or -- from the telecom infrastructure 406 in order to display on the display unit 430.

[0051]

the computer system 400 -- the main memory 408 -- it can also have random access memory (RAM) preferably, and can also have the auxiliary memory 410. As the auxiliary memory 410, the removable memory drive 414 showing the hard disk drive 412 and/or a floppy (registered trademark) disk drive, a magnetic tape drive, an optical disk drive, etc. can be mentioned, for example. The removable memory drive 414 is read with a known form to the removable storage unit 418, and/or writes in. The removable storage unit 418 expresses a floppy (registered trademark) disk, magnetic tape, an optical disc, etc. which are written by the removable memory drive 414. The removable storage unit 418 contains the computer usable storage with which computer software and/or data are memorized so that I may be understood.

[0052]

According to a substitute embodiment, the auxiliary memory 410 can contain other same devices that make a computer program or other commands load to the computer system 400. As such a device, the removable storage unit 422 and the interface 420 can be mentioned. As such an example, a program cartridge and a cartridge interface (what is seen by the video game device), Removable memory chips (eliminable programmable read-only memory (EPROM) or programmable read-only memory (PROM) etc.) and a related socket, And the interface 420 which makes other removable storage units 422, software, and data transmit to the computer system 400 from the removable storage unit 422 can be mentioned.

[0053]

The computer system 400 can also be provided with the communication interface 424. The communication interface 424 makes software and data transmit between the computer system 400 and an external device. As an example of the communication interface 424, a modem, network interfaces (Ethernet (registered trademark) card etc.), a communication port, the Personal Computer Memory Card International Association (PCMCIA) slot, a card, etc. can be mentioned. The software and data which are transmitted via the communication interface 424 are a gestalt of the signal 428 which can be an electronic signal, an electromagnetism signal, a lightwave signal, or other signals receivable with the communication interface 424. The communication interface 424 is provided with these signals 428 via the communication path (for example, channel) 426. This channel 426 can convey the signal 428 and can carry it out using a wire or a cable, an optical fiber, a telephone line, a cellular link, a radio frequency (RF) link, and other communications channels.

[0054]

In this specification, it is used in order to point out widely the medium of the hard disk which drove [removable memory] the term of a "computer program medium" and a "computer usable medium" 414, and was installed in the hard disk drive 412, and signal 428 grade. These computer program products provide the computer system 400 with software. This invention targets such a computer program product.

[0055]

A computer program (called computer control logic) is memorized by the main memory 408 and/or the auxiliary memory 410. A computer program is also receivable via the communication interface 424. If such a computer program is executed, it will enable it to perform the feature of this invention which the computer system 400 considered in this specification. If especially a computer program is executed, the processor 404 will enable it to perform the feature of this invention. Therefore, such a computer program expresses the controller of the computer system 400.

[0056]

In the embodiment by which this invention is carried out using software. Software is memorized by the computer program product and can be loaded to the computer system 400 using the removable memory drive 414, the hard drive 412, or the communication interface 424. If control logic (software) is performed by the processor 404, it will perform the function of this invention stated to the processor 404

in this specification.
[0057]
According to another embodiment, this invention is mainly carried out by hardware, for example using hardware components, such as an application-specific integrated circuit (ASIC). It will become clear in a person skilled in the art to carry out hardware state machinery so that the function described in this specification may be performed.
[0058]
According to another embodiment, this invention is carried out using the combination of both hardware and software.
[0059]
VI. Conclusion
Although mentioned above about the various embodiments of this invention, please understand that these are shown not as limitation but as an example. Probably, it will be clear to a person skilled in the art that a gestalt is performed and various detailed change can be made, without deviating from the pneuma and the range of this invention. Therefore, this invention should be limited by neither of the above-mentioned illustration embodiment, but only by following the following claim and its equivalent, it should be specified.
[Brief Description of the Drawings]
[0060]
[Drawing 1]It is a block diagram showing the local-area computer network of the company which can carry out this invention by one embodiment.
[Drawing 2]It is a flow chart which shows the network asset tracking process by the embodiment of substitution of this invention.
[Drawing 3 A] It is a flow chart which shows the network asset tracking process by the embodiment of substitution of this invention.
[Drawing 3 B] It is a flow chart which shows the network asset tracking process by the embodiment of substitution of this invention.
[Drawing 3 C] It is a flow chart which shows the network asset tracking process by the embodiment of substitution of this invention.
[Drawing 3 D] It is a flow chart which shows the network asset tracking process by the embodiment of substitution of this invention.
[Drawing 4]It is a block diagram of an illustration computer system useful to operation of this invention.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

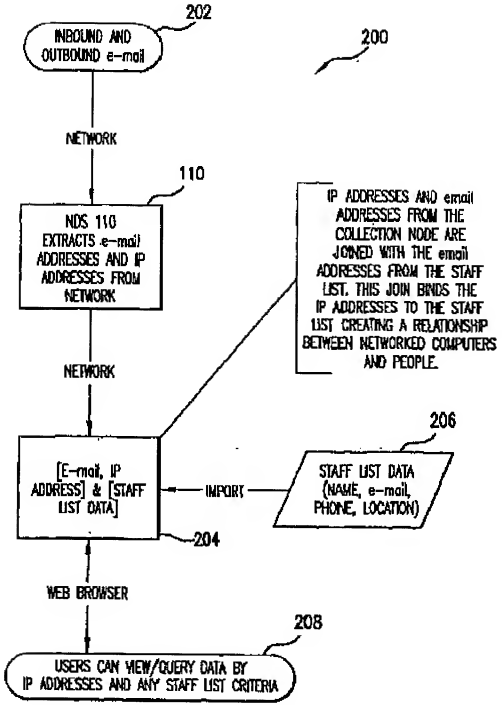
[Claim(s)]
[Claim 1]
It is a system which specifies a user of two or more computers in a communication network,
A database which memorizes directory information of two or more users who have obtained permission which uses said two or more computers in said communication network,
A name discovery device which has at least one connection with a primary switch in said communication network, and catches an inbound outbound electronic mail traffic,
It is a server which is connected to this name discovery device and can access said database via said communication network, Said directory information memorized by said inbound outbound electronic mail traffic caught by said name discovery device and said database is tied up, A server which has a server process which can specify any of two or more of said users are using any of two or more of said computers by it,
A system which specifies a user of two or more computers in preparation **********.
[Claim 2]
A system by which said communication network specifies a user of two or more computers in the communication network according to claim 1 which are Local Area Networks.
[Claim 3]
A system by which said Local Area Network specifies a user of two or more computers in the communication network according to claim 2 which are Ethernet (registered trademark) networks.
[Claim 4]
A system by which said communication network specifies a user of two or more computers in the communication network according to claim 1 which are wide area networks.
[Claim 5]
. Have further a central repository said name discovery device and said web server remember a said inbound [which was caught by said name discovery device] outbound [it is accessible and] electronic mail traffic to be. A system which specifies a user of two or more computers in the communication network according to claim 1.
[Claim 6]
A system by which said database specifies a user of two or more computers in the communication network according to claim 1 which are the ITU-T X.500 format databases.
[Claim 7]
The following data fields relevant to said two or more users in said database, Namely, an initial of a (i) first name, a (ii) last name, and a (iii) middle name, (iv) Nickname, a (v) alias, a (vi) building, a (vii) room, (viii) eternal E-mail and (ix) -- a system which specifies a user of two or more computers in the communication network according to claim 1 containing at least one of temporary E-mail, a (x) user name, a (xi) E-mail address, and (xii) affiliation / organizations.
[Claim 8]
. It is a web server process which can specify any of two or more of said users said server process

answers an inquiry of a browser base, and are using any of two or more of said computers. A system which specifies a user of two or more computers in the communication network according to claim 1.
[Claim 9]
Said inbound outbound electronic mail traffic caught by said name discovery device The following, Namely, a system which specifies a user of two or more computers in the communication network according to claim 1 containing at least one of a (i)POP electronic mail traffic, a (ii)IMAP electronic mail traffic, and (iii)SMTP electronic mail traffics.
[Claim 10]
It is how to specify a user of two or more computers in a communication network,
A step which catches an inbound outbound electronic mail traffic from at least one primary switch in said communication network,
A step which extracts an Internet protocol address and an e-mail address from said caught inbound outbound electronic mail traffic,
It is a step which accesses a database of directory information of two or more users who have obtained permission which uses said two or more computers in said communication network, A step in which this database contains two or more e-mail addresses which correspond to one of said two or more users, respectively and to access,
It is a step which connects said extracted e-mail address to said two or more e-mail addresses memorized by said database, A step which maps a subset of said extracted Internet protocol address in two or more of said users' subset by it and to tie up,
How to specify a user of two or more computers in ****** and a communication network.
[Claim 11]
How to specify a user of two or more computers in the communication network according to claim 10 which contain further a step which memorizes said extracted Internet protocol address and an e-mail address to a central repository.
[Claim 12]
A step which accesses said central repository,
A step in which it is a step which generates a data file with a predetermined time interval, and said data file includes information about any of two or more of said users used any of two or more of said computers into said predetermined time interval and to generate,
How to specify a user of two or more computers in the communication network according to claim 11 included in a pan.
[Claim 13]
Said step to extract,
It is a step which uses pattern matching based on a known electronic mail protocol, A step which extracts said Internet protocol address and said e-mail address from said caught inbound outbound electronic mail traffic by it and to be used
How to specify a user of two or more computers in ****** and the communication network according to claim 10.
[Claim 14]
A way said known electronic mail protocol specifies a user of two or more computers in the communication network according to claim 13 which are one of the following protocols, i.e., (i)POP, (ii) IMAP, and (iii)SMTP.
[Claim 15]
A method of specifying a user of two or more computers in the communication network according to claim 10 that said communication network is a Local Area Network.
[Claim 16]
A method of specifying a user of two or more computers in the communication network according to claim 15 that said Local Area Network is an Ethernet (registered trademark) network.
[Claim 17]
A method of specifying a user of two or more computers in the communication network according to

claim 10 that said communication network is a wide area network.
[Claim 18]
A method of specifying a user of two or more computers in the communication network according to claim 10 that said database is the ITU-T X.500 format database.
[Claim 19]
A step which specifies one user in said two or more computers in said communication network via said communication network and which receives an inquiry including an Internet protocol address,
A step which uses said mapping to said subset of two or more of said users of said subset of said extracted Internet protocol address, and answers said inquiry using said received Internet protocol address,
How to specify a user of two or more computers in the communication network according to claim 10 included in a pan.
[Claim 20]
A data field of the following to which said database is related with each of two or more of said users, Namely, an initial of a (i) first name, a (ii) last name, and a (iii) middle name, (iii) How to specify a user of two or more computers in the communication network according to claim 10 which contain further at least one of nickname, a (iv) alias, a (v) building, a (vi) room, a (vii) user name, and (viii) affiliation / organizations.
[Claim 21]
A step which receives an inquiry which contains at least one of said data fields which specify one user in said two or more computers in said communication network via said communication network,
A step which uses said mapping to said subset of two or more of said users of said subset of said extracted Internet protocol address, and answers said inquiry using said at least one of said data fields received,
How to specify a user of two or more computers in the communication network according to claim 20 included in a pan.
[Claim 22]
It is a computer program product containing a computer usable medium which memorized control logic which makes a user of two or more terminals in a communication network specify it as a computer, and is said control logic,
The 1st computer-readable program code means that makes said computer catch an inbound outbound electronic mail traffic from at least one primary switch in said communication network,
The 2nd computer-readable program code means that makes said computer extract an Internet protocol address and an e-mail address from said caught inbound outbound electronic mail traffic,
It is the 3rd computer-readable program code means made to access a database of directory information of two or more users who have obtained permission which uses said two or more terminals in said communication network for said computer, 3rd computer-readable program code means by which said database contains two or more e-mail addresses which correspond to one of said two or more users, respectively,
Said computer is made to connect said extracted e-mail address to said two or more e-mail addresses memorized by said database, The 4th computer-readable program code means that makes two or more of said users' subset map a subset of said extracted Internet protocol address by it,
******, a computer program product.
[Claim 23]
The computer program product according to claim 22 which contains further the 5th computer-readable program code means that makes a central repository memorize said extracted Internet protocol address and an e-mail address in said computer.
[Claim 24]
The 6th computer-readable program code means that makes said central repository access said computer,
To said computer, with a predetermined time interval, are a data file the 7th computer-readable program

code means made to create, and said data file, The 7th computer-readable program code means including information about any of two or more of said users used any of two or more of said terminals into said predetermined time interval,
The computer program product according to claim 23 included in a pan.
[Claim 25]
Said 2nd computer-readable program code means,
Said computer is made to perform pattern matching based on a known electronic mail protocol, The 5th computer-readable program code means that makes said Internet protocol address and said e-mail address extract from said caught inbound outbound electronic mail traffic
******, the computer program product according to claim 22.
[Claim 26]
The computer program product according to claim 25 in which said known electronic mail protocol is one of the following protocols, i.e., (i)POP, (ii)IMAP, and (iii)SMTP.
[Claim 27]
The computer program product according to claim 22 in which said database is the ITU-T X.500 format database.
[Claim 28]
5th computer-readable program code means that makes an inquiry including an Internet protocol address receive to specify one user in said two or more terminals in said communication network as said computer via said communication network,
Said mapping to said subset of two or more of said users of said subset of said extracted Internet protocol address is used for said computer, The 6th computer-readable program code means made to answer said inquiry using said received Internet protocol address,
The computer program product according to claim 22 included in a pan.
[Claim 29]
A data field of the following to which said database is related with each of two or more of said users, Namely, an initial of a (i) first name, a (ii) last name, and a (iii) middle name, (iii) The computer program product according to claim 22 which contains ****** for at least one of nickname, a (iv) alias, a (v) building, a (vi) room, a (vii) user name, and (viii) affiliation / organizations.
[Claim 30]
Even if small [of said data fields which specify one user in said two or more terminals in said communication network as said computer via said communication network]
The 5th computer-readable program code means that makes an inquiry containing one receive,
Said mapping to said subset of two or more of said users of said subset of said extracted Internet protocol address is used for said computer, The 6th computer-readable program code means made to answer said inquiry using said at least one of said said received data fields received,
The computer program product according to claim 29 included in a pan.

[Translation done.]


202
INBOUND AND OUTBOUND e-mail
200
NETWORK
110
NDS 110 EXTRACTS e-mail ADDRESSES AND IP ADDRESSES FROM NETWORK
IP ADDRESSES AND email ADDRESSES FROM THE COLLECTION NODE ARE JOINED WITH THE email ADDRESSES FROM THE STAFF LIST. THIS JOIN BINDS THE IP ADDRESSES TO THE STAFF LIST CREATING A RELATIONSHIP BETWEEN NETWORKED COMPUTERS AND PEOPLE.
NETWORK
206
[E-mail, IP ADDRESS] & [STAFF LIST DATA]
IMPORT
STAFF LIST DATA (NAME, e-mail, PHONE, LOCATION)
204
WEB BROWSER
208
USERS CAN VIEW/QUERY DATA BY IP ADDRESSES AND ANY STAFF LIST CRITERIA

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

WRITTEN AMENDMENT

[A written amendment]
[Filing date]April 18 (2006.4.18), Heisei 18
[The amendment 1]
[Document to be Amended]Claim
[Item(s) to be Amended]Whole sentence
[Method of Amendment]Change
[The contents of amendment]
[Claim(s)]
[Claim 1]
It is a system which specifies a user of two or more computers in a communication network of an organization by matching user identification information from directory information of an organization with user identification information and the present Internet protocol address from which it was extracted by a discovery device,
A database which memorizes directory information of said organization which does not include a list of devices although user identification information is included,
A discovery device which has at least one connection with said switch for monitoring passively traffic which passes a switch in said communication network, and extracts user identification information and a corresponding Internet protocol address,
It is a server which is connected to said discovery device and can access said database via said communication network, Said user identification information from directory information of said organization is matched with said user identification information and the present Internet protocol address from which it was extracted by said discovery device, A server with any of contact in directory information of said organization able to determine automatically whether to use each of said extracted Internet protocol address now
A ******** system.
[Claim 2]
Said communication network is a Local Area Network.
The system according to claim 1.
[Claim 3]
Said Local Area Network is an Ethernet (registered trademark) network.
The system according to claim 2.
[Claim 4]
A central repository which memorizes said accessible traffic by which said discovery device and a web server were monitored with said discovery device
The system according to claim 1 with which a pan is equipped.
[Claim 5]
Said database is a formatted database.
The system according to claim 1.

[Claim 6]
Said database contains the following data fields, i.e., (i) first name, last names and (ii) e-mail addresses, and/or user names.
The system according to claim 1.
[Claim 7]
Said server is a web server which can specify any of a user an inquiry of a browser base is answered and are using any of a computer.
The system according to claim 1.
[Claim 8]
Said database The following data fields, i.e., an initial of a (i) middle name, (ii) nickname, a (iii) alias, a (iv) building, a (v) room, and (vi) -- eternal E-mail and (vii) -- include further arbitrary combination of a data field of 1 of temporary E-mail, or (viii) affiliation / organizations or (ix) above-mentioned (i) - (viii)

The system according to claim 6.
[Claim 9]
It is how to specify a user of two or more computers in a communication network of an organization, by matching user identification information from directory information of an organization with user identification information and the present Internet protocol address from which it was extracted by a discovery device,
A step which monitors traffic which passes a switch in said communication network,
A step which extracts user identification information and a corresponding Internet protocol address from said monitored traffic,
A step which accesses a database of directory information of said organization which does not include a list of devices although user identification information is included,
Said user identification information from directory information of said organization is matched with said user identification information and the present Internet protocol address from which it was extracted by said discovery device, A step as which any of contact within directory information of said organization determine automatically whether each of said extracted Internet protocol address is used now Preparation ******.
[Claim 10]
A step which memorizes said user identification information and a corresponding Internet protocol address to a central repository
A method according to claim 9 of equipping a pan.
[Claim 11]
A step which accesses said central repository,
A step which generates a data file including information about any of a user used any of a computer into a predetermined time interval with said predetermined time interval
A method according to claim 10 of equipping a pan.
[Claim 12]
Said step to extract,
A step which extracts an e-mail address and/or a user name, and a corresponding Internet protocol address from said monitored traffic by using pattern matching based on a known electronic mail protocol and/or Challenge Handshake Authentication Protocol
A method according to claim 9 of ****(ing).
[Claim 13]
Said communication network is a Local Area Network.
A method according to claim 9.
[Claim 14]
Said Local Area Network is an Ethernet (registered trademark) network.
A method according to claim 13.
[Claim 15]

Said database is a formatted database.
A method according to claim 9.
[Claim 16]
A step which receives an inquiry which specifies a user of a computer in said communication network, and including an Internet protocol address via said communication network,
A step which answers said inquiry using said received Internet protocol address using said matching with a subset of said extracted Internet protocol address, and two or more users' subset
A method according to claim 9 of equipping a pan.
[Claim 17]
Said database contains the following data fields, i.e., (i) first name, last names and (ii) e-mail addresses, and/or user names.
A method according to claim 9.
[Claim 18]
A step which receives an inquiry which contains at least one of said data fields which specify a user of a computer in said communication network via said communication network,
A step which answers said inquiry using a received data field using said matching with a subset of said extracted Internet protocol address, and two or more users' subset
A method according to claim 17 of equipping a pan.

[Translation done.]